Using the Australian Government Information Security Manual

Applying a risk-based approach to cyber security

Assess security controls

- Minor grammar changes and a change in content to note that ASD assessors (or their delegates) are able to conduct security assessments for TOP SECRET systems, including sensitive compartmented information systems.

Guidelines for Cyber Security Roles

Chief Information Security Officer

Required skills and experience

- Introduction of new content.

  The role of the Chief Information Security Officer (CISO) requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. Additionally, CISOs must adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies. It is expected that CISOs show innovation and imagination in conceiving and delivering cyber security strategies for their organisations.

Providing cyber security leadership and guidance

- Change of title from ‘cyber security leadership’ to ‘providing cyber security leadership and guidance’.

- Minor grammar changes to content.

- Security control 0714 was amended to capture a CISO’s role in providing cyber security guidance for their organisation.

  Security Control: 0714; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
  A CISO is appointed to provide cyber security leadership for their organisation.

  Security Control: 0714; Revision: 5; Updated: Oct-20; Applicability: O, P, S, TS
  A CISO is appointed to provide cyber security leadership for their organisation.
A CISO is appointed to provide cyber security leadership and guidance for their organisation.

**Overseeing the cyber security program**

- Change title from ‘responsibilities’ to ‘overseeing the cyber security program’.
- Security control 1478 was amended to remove overlap with security control 0714 and to focus on a CISO’s role in overseeing their organisation’s cyber security program.

  **Security Control: 1478; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS**
  The CISO provides strategic-level guidance for their organisation’s cyber security program and ensures their organisation’s compliance with cyber security policy, standards, regulations and legislation.

  **Security Control: 1478; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS**
  The CISO oversees their organisation’s cyber security program and ensures their organisation’s compliance with cyber security policy, standards, regulations and legislation.

- Security control 1617 was introduced to capture the ongoing maintenance of an organisation’s cyber security program.

  **Security Control: 1617; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS**
  The CISO regularly reviews and updates their organisation’s cyber security program to ensure its relevance in addressing cyber threats and harnessing business cyber opportunities.

- Security control 0724 was reintroduced and amended slightly.

  **Control: 0724; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should**
  The CISO should implement information security measurement metrics and key performance indicators.

  **Security Control: 0724; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS**
  The CISO implements cyber security measurement metrics and key performance indicators for their organisation.

**Coordinating cyber security**

- Introduction of new content.

  The CISO is responsible for ensuring the alignment of cyber security and business objectives within their organisation. To achieve this, they should facilitate communication between cyber security and business stakeholders. This includes translating cyber security concepts and language into business concepts and language as well as ensuring that business teams consult with cyber security teams to determine appropriate security measures when planning new business projects. Additionally, as the CISO is responsible for the development of the strategic-level cyber security program, they are best placed to advise projects on the strategic direction of cyber security.

- Security control 0725 was reintroduced and amended slightly.

  **Control: 0725; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should**
  The CISO should facilitate information security and business alignment, and communication through an information security steering committee or advisory board which meets formally and on a regular basis.

  **Security Control: 0725; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS**
  The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key business and ICT executives, which meets formally and on a regular basis.

- Security control 0726 was reintroduced and amended slightly.

  **Control: 0726; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should**
  The CISO should coordinate security risk management projects between business and information security teams.
The CISO coordinates security risk management activities between cyber security and business teams.

**Reporting on cyber security**

- Introduction of new content.
  
  The CISO is responsible for directly reporting cyber security matters to their organisation’s senior executive and/or Board. Reporting should cover:
  
  - the organisation’s security risk profile
  - the status of key systems and any outstanding security risks
  - any planned cyber security uplift activities
  - any recent cyber security incidents
  - expected returns on cyber security investments.

  Reporting on cyber security matters should be structured by business functions, regions or legal entities and support a consolidated view of the organisation’s cyber security risks.

  It is important that the CISO is able to translate cyber security risks into operational risks for the organisation, including financial and legal risks, in order to enable more holistic conversations about the organisation’s risks.

- Security control 0718 was reintroduced and amended slightly.

  Control: 0718; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should
  The CISO should report to the agency head on information security issues.

  Security Control: 0718; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO reports directly to their organisation’s senior executive and/or Board on cyber security issues.

**Overseeing incident response activities**

- Introduction of new content.

  To ensure the CISO is able to accurately report to their organisation’s senior executive and/or Board on cyber security matters, it is important they are fully aware of all cyber security incidents within their organisation.

  The CISO is also responsible for overseeing their organisation’s response to cyber security incidents, including how internal teams respond and communicate with each other during an incident. In the event of a major cyber security incident, the CISO should be prepared to step into a crisis management role. They should understand how to bring clarity to the situation and communicate effectively with internal and external stakeholders.

- Security control 0733 was reintroduced and amended slightly.

  Control: 0733; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should
  The CISO should be fully aware of all cyber security incidents.

  Security Control: 0733; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO is fully aware of all cyber security incidents within their organisation.

- Security control 1618 was introduced to capture the role that a CISO has in overseeing incident response activities for their organisation.

  Security Control: 1618; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO oversees their organisation’s response to cyber security incidents.
Contributing to business continuity and disaster recovery planning

- Introduction of new content.

  The CISO is responsible for contributing to the development and maintenance of their organisation’s business continuity and disaster recovery plan, with the aim to improve business resilience and ensure the continued operation of critical business processes. Other senior executives may also be responsible for contributing to the development and maintenance of the business continuity and disaster recovery plan.

- Security control 0734 was reintroduced and amended slightly.

  Control: 0734; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should
  The CISO should coordinate the development of disaster recovery policies and standards to ensure that business-critical services are supported appropriately in the event of a disaster.

  Security Control: 0734; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO contributes to the development and maintenance of a business continuity and disaster recovery plan for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.

Developing a cyber security communications strategy

- Introduction of new content.

  To facilitate broad security cultural change across their organisation, the CISO should act as a thought leader continually communicating their strategy and vision. A communication strategy can be helpful in achieving this. Communications should be tailored to different parts of the organisation and be topical for the intended audience.

- Security control 0720 was reintroduced and amended slightly.

  Control: 0720; Revision: 0; Updated: Sep-09; Applicability: G, P, C, S, TS; Compliance: should
  The CISO should be responsible for the development of an information security communications plan.

  Security Control: 0720; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO develops and maintains a cyber security communications strategy for their organisation.

Working with suppliers and service providers

- Introduction of new content.

  The CISO is responsible for ensuring that a consistent vendor management process is applied across their organisation, from discovery through to ongoing management. As supplier and service provider relationships come with additional security risks for their organisation, the CISO should assist personnel with assessing cyber supply chain risks and understand the security impacts of entering into contracts with suppliers and service providers.

- Security control 0731 was reintroduced and amended slightly.

  Control: 0731; Revision: 1; Updated: Nov-10; Applicability: G, P, C, S, TS; Compliance: should
  The CISO should coordinate the use of external information security resources including contracting and managing the resources.

  Security Control: 0731; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
  The CISO oversees cyber supply chain risk management activities for their organisation.

Receiving and managing a dedicated cyber security budget

- Introduction of new content.
Receiving and managing a dedicated cyber security budget will ensure the CISO has sufficient access to funding to support their cyber security program, including cyber security uplift activities and responding to cyber security incidents.

- Security control 0732 was reintroduced and amended slightly.
  
  **Control:** 0732; **Revision:** 1; **Updated:** Nov-10; **Applicability:** G, P, C, S, TS; **Compliance:** should
  
  The CISO should control the information security budget.

- Security control 0732; **Revision:** 2; **Updated:** Oct-20; **Applicability:** O, P, S, TS
  The CISO receives and manages a dedicated cyber security budget for their organisation.

**Overseeing cyber security personnel**

- Introduction of new content.
  
  The CISO is responsible for the cyber security workforce within their organisation, including plans to attract, train and retain cyber security personnel in order to ensure that sufficient resources are in place to perform cyber security functions. CISOs should delegate relevant tasks to cyber security managers and other personnel as required and provide them with adequate authority and resources to perform their duties.

- Security control 0717 was reintroduced and amended slightly.
  
  **Control:** 0717; **Revision:** 1; **Updated:** Nov-10; **Applicability:** G, P, C, S, TS; **Compliance:** should
  
  The CISO should be responsible for overseeing the management of information security personnel.

- Security control 0717; **Revision:** 2; **Updated:** Oct-20; **Applicability:** O, P, S, TS
  The CISO oversees the management of cyber security personnel within their organisation.

**Overseeing cyber security awareness raising**

- Introduction of new content.
  
  To ensure personnel are actively contributing to the security posture of their organisation, a cyber security awareness training program should be developed. As the CISO is responsible for cyber security within their organisation, they should oversee the development and operation of the program.

- Security control 0735 was reintroduced and amended slightly.
  
  **Control:** 0735; **Revision:** 1; **Updated:** Nov-10; **Applicability:** G, P, C, S, TS; **Compliance:** should
  
  The CISO should oversee the development and operation of information security awareness and training programs.

- Security control 0735; **Revision:** 2; **Updated:** Oct-20; **Applicability:** O, P, S, TS
  The CISO oversees the development and operation of their organisation’s cyber security awareness training program.

**System owners**

- The ‘responsibilities’ content was split into three different content blocks: ‘gaining authorisation to operate systems’, ‘monitoring cyber threats, security risks and security controls’ and ‘annual reporting of system security status’ to more closely align with the security controls that they relate to.
Guidelines for Cyber Security Incidents

Detecting cyber security incidents

The content was amended to move the information relating to the use of security software and appliance logs from the paragraph below the table into the table.

Guidelines for System Hardening

Operating system hardening

Operating system configuration

- Security control 1491 was amended to cover the use of all script engines, not just those native to Microsoft Windows.

  Security Control: 1491; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
  Standard users are prevented from running all script execution engines shipped with Microsoft Windows including Windows Script Host (cscript.exe and wscript.exe), powershell.exe, powershell_ise.exe, cmd.exe, wmic.exe and Microsoft HTML Application Host (mshta.exe).

  Security Control: 1491; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
  Standard users are prevented from running script execution engines in Microsoft Windows, including:
  - Windows Script Host (cscript.exe and wscript.exe)
  - PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)
  - Command Prompt (cmd.exe)
  - Windows Management Instrumentation (wmic.exe)
  - Microsoft HTML Application Host (mshta.exe).

PowerShell

- Introduction of new content.

PowerShell is a powerful scripting language developed by Microsoft to provide an integrated interface for automated system administration, and is an important part of system administrator toolkits due to its ubiquity and the ease with which it can be used to fully control Microsoft Windows environments. However, it is also a dangerous exploitation tool in the hands of an adversary. In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, PowerShell 2.0 and below should be removed from operating systems. Additionally, PowerShell’s language mode should be set to Constrained Language Mode to achieve a balance between functionality and security. Finally, logging functionality available in PowerShell, such as module logging, script block logging and transcription, can provide invaluable information for incident responders following cyber security incidents that involved PowerShell being used for malicious purposes.

- Security control 1621 was introduced to cover the removal of PowerShell 2.0 and below from operating systems.

  Security Control: 1621; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell 2.0 and below is removed from operating systems.

- Security control 1622 was introduced to cover the use of Constrained Language Mode for PowerShell.
  
  **Security Control: 1622; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS**
  **PowerShell is configured to use Constrained Language Mode.**

- Security control 1623 was introduced to cover the use of PowerShell logging functionality.
  
  **Security Control: 1623; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS**
  **PowerShell is configured to use module logging, script block logging and transcription functionality.**

- Security control 1624 was introduced to cover the protection of Windows Event Logs that potentially contain sensitive information from PowerShell’s script block logging functionality.
  
  **Security Control: 1624; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS**
  **PowerShell script block logs are protected by Protected Event Logging functionality.**

Further information

- The content was amended to include additional information on using PowerShell.


  Further information on implementing PowerShell logging is available at [https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html](https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html) and [https://devblogs.microsoft.com/powershell/powershell-the-blue-team/](https://devblogs.microsoft.com/powershell/powershell-the-blue-team/).

**Authentication hardening**

**Setting and resetting credentials for user accounts**

- Change of content title from ‘setting and resetting credentials’ to ‘setting and resetting credentials for user accounts’.

**Setting and resetting credentials for service accounts**

- Introduction of new content.

  To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts in Microsoft Windows Server 2012. In doing so, service accounts that are created as group Managed Service Accounts do not require manual credential management by administrators, as the operating system automatically manages the credentials. This ensures that service account credentials are not misplaced or forgotten, and that they are automatically changed on a regular basis.

- Security control 1619 was introduced to recommend the use of group Managed Service Accounts to manage credentials for service accounts.
  
  **Security Control: 1619; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS**
  **Service accounts are created as group Managed Service Accounts.**

**Unsecure authentication methods**

- The content was rewritten to include discussion on NT LAN Manager and Kerberos authentication methods.

  Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, Local Area Network (LAN) Manager and NT LAN Manager authentication...
methods use weak hashing algorithms. As such, passwords/passphrases used as part of LAN Manager authentication and NT LAN Manager authentication (i.e. NTLMv1, NTLMv2 and NTLM2) can easily be compromised. Instead, organisations should use Kerberos for authentication within Microsoft Windows environments.

- Security control 1055 was amended to recommend disabling NT LAN Manager authentication methods (i.e. NTLMv1, NTLMv2 and NTLM2) in addition to the LAN Manager authentication method.

Security Control: 1055; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
LAN Manager is disabled for password/passphrase authentication.

Security Control: 1055; Revision: 4; Updated: Oct-20; Applicability: O, P, S, TS
LAN Manager and NT LAN Manager authentication methods are disabled.

- Security control 1620 was introduced to reflect the recommendation within the ACSC’s Security Administration publication that privileged accounts be members of the Protected Users security group.

Security Control: 1620; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
Privileged accounts are members of the Protected Users security group.

Please note: There is no requirement for organisations to be compliant with every monthly update to the Australian Government Information Security Manual (ISM). Instead, organisations are encouraged to review the security risks for their systems (using the latest version of the ISM available at the time) based on a frequency suitable for their business requirements and in accordance with their corporate risk management framework. Further information on applying the ISM can be found in the Using the Australian Government Information Security Manual chapter.